PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of:	Tara Chand Singhal	)
Serial No:	09/891,913	) Art Unit 3692
Filed:	06/26/2001	)
For:	Method and Apparatus for A Payment Card System	)
Examiner:	Monfeldt, Sarah M.	)
Attorney Docket:	11195.33	)

APPEAL BRIEF

Commissioner for Patents

P O Box 1450, Alexandria, VA 22313-1450

Dear Sir:

This appeal brief, a transmittal form, and required fee of $270.00 are enclosed. The Notice of Appeal was filed 02/02/2010 on the Final office action dated 11/24/2009 and the claims have been twice rejected as required under 37 CFR §41.31.

The appeal is timely filed with in the two months statutory period of the Notice of Appeal, and contains the ten items under appropriate headings and in order as required under 37 CFR §41.37 Appellant's brief.

It should be noted that the Appellant is the applicant/inventor pro se and is not a registered practitioner.

CERTIFICATE OF MAILING UNDER 37 CFR §1.8

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail, postage prepaid, in an envelope addressed to: Mail Stop: Appeal Brief, Commissioner for Patents, P O Box 1450, Alexandria, VA 22313-1450, on March 29 /2010 by

T Singhal TARA CHAND SINGHAL, Applicant

04/01/2010 HDESTA1 00000026 09891913

01 FC:2402 270.00 OP

APPEAL BRIEF

TABLE OF CONTENTS

(1) REAL PARTY IN INTEREST

Tara Chand Singhal, applicant/inventor

(2) RELATED APPEALS AND INTERFERENCES

None

(3) STATUS OF CLAIMS

Claims 1-105 have been canceled without prejudice. Claims 106 to 124 have been rejected in a Final Office Action dated 11/24/2009. Claims 106-124 are pending in the Application and are the subject of this appeal.

(4) STATUS OF AMENDMENTS

No Amendments after final office action rejection dated 11/24/2009 have been filed.

(5) SUMMARY OF CLAIMED SUBJECT MATTER

The embodiments of a payment card system provide security of the customer identity data and bankcard data from the merchant computer systems themselves when the customer uses bankcards at merchant sales terminals for payment transactions from the customer to the merchant.

To achieve this objective, of protecting the customer private data from the merchant systems themselves, whereas that is unachievable in the prior art bankcard payment transactions at the merchant systems, because the merchant point of sale systems create a payment authorization request record that contains (i) the customer identity and bankcard data, (ii) meta data of, date, time, and reference number, and (iii) merchant terminal identifier, for submission to a card authorization network for routing to the card-issuing banks via a merchant gateway, thus the merchant systems by necessity require the customer identity and bankcard data for be able to complete a payment authorization request record data as above, the

claimed subject matter achieves that objective by using three unique elements, working in conjunction with each other.

One of these elements is a physical plastic payment card (not a bankcard) that resembles prior art bankcards. This payment card element does not contain anywhere on the payment card, customer identity data. The payment card only has an encoded customer identifier without identity data that is meaningful only to a payment card system. **[Ref., page 6, line 29 to page 7, line 10]**

The second element, is an adapted prior art merchant gateway. A prior art merchant gateway is a router mechanism that routes the bankcard driven payment authorization request to the various card-issuing banks using the first four digits of the bankcard number that identifies the card-issuing bank.

The adapted prior art merchant gateway of the claimed subject matter adapts a prior art merchant gateway by providing a new logic and a new interface in the merchant gateway. The new logic filters the payment card transactions from other bankcard transactions and for these payment card transactions uses the new gateway interface to interface with an independent payment card system, which stores the actual customer bankcard data. The new logic and the new interface in the adapted merchant gateway sends the customer-identifier to the payment card system and receives the actual customer bankcard data for the specific transaction. The adapted gateway, on receiving the actual customer bankcard data, then assembles and completes a prior art payment authorization request record for submission to the card-issuing banks. **[Ref., page 8, lines 28 to page 9, line 21]**

The third element is the payment card system that has a customer identifier that is without customer identity data, the customer identifier maps to a plurality of bankcard data of the customer in the payment card system. The customer identifier is encoded to be an encoded customer identifier when encoded with an algorithm from a list of such algorithms in a database maintained by the payment card system

and then embeds a reference code that references the algorithm, the encoded customer identifier is then encoded on a payment card encoding mechanism, wherein the payment card and the CPIN is used by the customer at a merchant point of sale (POS) of a merchant system for conducting a payment transaction. **[Ref., page 17, line 24 to page 18, line 2]**

Using these three elements, the payment card system of the claimed subject matter enables payment to merchants without having to distribute and copy customer identity and bankcard data to their record and systems, from where it has been subject to theft from their systems as had been covered in many news items. Instead the customer identity and bankcard data is stored in an encrypted form in a central payment card system and decrypted for use at the time of the actual payment transactions.

Further, the payment card system of the claimed subject matter, as described above operates within the existing payment infrastructure that includes the merchant point of sale systems and the card-issuing banks, without changing their operation or interfaces. Hence the operation of the payment card system is transparent to both the merchant sales systems and the card-issuing banks.

Concise explanation of subject matter in claims involved in the appeal:

The following states a concise explanation of the subject matter defined in each of the independent claims involved in the appeal. The independent claims are: 106, 109, 114, and 123, for which a concise explanation is being identified here by reference to page number, line number, and Figure number and by references numbers where applicable.

Claim 106

The claim teaches a method of protecting from theft and misuse bankcard data from merchant computer systems and securely selecting any one of a plurality of bankcards of a customer at a merchant point of sale interface for a payment transaction to a merchant comprising the steps of:

a. enabling selecting a debit card transaction requiring entry of a PIN in a merchant point of sale (POS) interface, enabling entering of (i) a customer identifier, without customer identity data, by a payment card that encodes the customer identifier and (ii) a bankcard specific personal identification number (CPIN) in the merchant point of sale (POS) interface; **[Ref., page 7, lines 20 to page 9, line 21]**

b. enabling sending the customer identifier and the CPIN to an adapted prior art merchant gateway, along with the payment transaction data that includes a merchant identifier and a payment amount; **[Ref., page 7, lines 20 to page 9, line 21]**

c. interfacing by the adapted prior art merchant gateway with a payment card system, and sending to the payment card system the customer identifier and the CPIN; **[Ref., page 7, lines 20 to page 9, line 21]**

d. having stored customer bankcard data in the payment card system, wherein, each bankcard is identified with a separate CPIN, identifying a particular bankcard data of the customer and verifying the customer by the bankcard specific CPIN in the payment card system; **[Ref., page 7, lines 20 to page 9, line 21]**

e. returning to the adapted prior art merchant gateway the bankcard data corresponding to the customer identifier and the CPIN from the payment card system; **[Ref., page 7, lines 20 to page 9, line 21]**

f. assembling by the adapted prior art merchant gateway, a payment transaction record to include the bankcard data from the payment card system and the payment transaction data, and by submitting the payment transaction record to a bankcard authorization network, wherein the method does not transfer bankcard identity data to the merchant computer systems. **[Ref., page 7, lines 20 to page 9, line 21]**

Claim 109:

The claim teaches a payment card system and that protects private data of a customer from theft and misuse from merchant computer systems in customer to merchant payment transactions, comprising:

a. a payment card with a substrate; **[Ref., page 6, line 29 to page 7, line 10]**

b. a customer identifier that is without customer identity data, the customer identifier maps to the payment card system; **[Ref., page 16, line 10 to line 16]**

c. the customer identifier is encoded to be an encoded customer identifier when the customer identifier is encoded with an algorithm in the payment card system and then embeds a reference code that references the algorithm; **[Ref., page 17, line 24 to page 18, line 2]**

d. the substrate encoded with the encoded customer identifier and the substrate printed with an alias name selected by the customer. **[Ref., page 18, line 21 to page 20, line 10, and page 16, line 10 to line 16]**

Claim 114:

This claim teaches a method of conducting a payment transaction that protects the privacy of customer identity and bankcard data, from theft and misuse from merchant computer systems, having the steps of:

a. enabling creating a customer identifier that is without customer identity data, the customer identifier maps to a payment card system; **[Ref., page 16, line 10 to page 18, line 2]**

b. encoding the customer identifier with an algorithm, and then embedding a reference code that references the algorithm in the payment card system, thus getting an encoded customer identifier; **[Ref., page 17, line 24 to page 18, line 2]**

c. delivering to a customer, a payment card with a substrate printed with an alias name selected by the customer and encoded with the encoded customer identifier. **[Ref., page 6, line 29 to page 7, line 10]**

Claim 123:

This claim teaches a payment security system that provides identity security in use of bankcards, from merchant computer systems, comprising:

a. a customer identifier that is without customer identity data; **[Ref., page 6, line 29 to page 7, line 10]**

b. the customer identifier maps to a plurality of bankcard data of the customer, each bankcard data identified with a card specific personal identification number (CPIN) in the payment security system; **[Ref., page 11, line 12 to page 13, line 16]**

c. the customer identifier is encoded to be an encoded customer identifier when encoded with an algorithm from a list of such algorithms in a database maintained by the payment security system and then embeds a reference code that references the algorithm, the encoded customer identifier is then encoded on a payment card encoding mechanism, wherein the payment card and the CPIN is used by the customer at a merchant point of sale (POS) of a merchant system for conducting a payment transaction. **[Ref., page 17, line 24 to page 18, line 2]**

(6) GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

GROUND #1:

Rejected claims 109-110, 112, 115-116, under 35 USC 103(a) as being unpatentable over Rose et al. Rejected claims 111, under 35 USC 103(a) as being unpatentable over Rose et al, in view of Campisano. Rejected claims 106-108, under 35 USC 103(a) as being unpatentable over Rose et al, in view of Campisano, further in view of Duyck and Low et al. Rejected claims 113, under 35 USC 103(a) as being unpatentable over Rose et al in view of Campisano and Low et al, claims 117, under 35 USC 103(a) as being unpatentable over Rose et al in view of Low et al. Rejected claims 118-120, under 35 USC 103(a) as being unpatentable over Rose et al in view of Albert and Duyck.

Rejected claim 121 over Rose in view of Albert, and Duyck, and in view of Campisano and Gillin et al, claim 122 over Rose in view of Albert, Duyck, Campisano and Gillin and Low et al, claim 124 over Rose in view of Campisano and Low et al.

Appellant submits such rejections are improper under 35 USC 103(a) and Graham v. Deere which governs determination of obviousness by the USPTO.

GROUND #2:

Examiner misunderstands and mis-cites KSR v. Teleflex, and its seven rationales to support 103 (a) rejections, under an obviousness enquiry.

GROUND #3:

Examiner misconstrues and misunderstands the nature and scope of the claimed subject matter" as used in the claims in light of the specification and thus has erred in applying the "Broadest reasonable construction" standard and as a basis for 103(a) obviousness rejection.

(7) ARGUMENT

GROUND #1:

Appellant's Arguments:

Rose and Campisano are the major or primary cited prior arts underlying all of these 103(a) rejections and hence would be analyzed first.

What Rose and Campisano teach and do not teach

The primary prior art cited for obviousness rejection by the examiner is Rose et al. Rose art is on a Rose payment card. Rose teaches different embodiments of the Rose payment card, as illustrated in Rose Figures 2 to 3A-E. These Rose embodiments cover from a blank card to a decorative card, to a card with or without a bank name, and a card where the customer can etch or write his name initials. These different embodiments do not display the customer name and or bankcard number. Rose et al further teaches a payment card, which has a code on the card. The code is associated with multiple bank accounts in a database at a remote location.

When the Rose payment card is used at an ATM/POS, the code from the card is read and routed to the database at the remote location. The database matches the code, and the database returns the identity of each account in the database to the ATM/POS to be displayed on the ATM/POS screen, along with the PIN of each account. The user is then asked to select from this list of accounts, a specific account to be used for this transaction and then asked to enter the corresponding PIN for that account in the ATM/POS. The ATM/POS logic itself then matches the entered PIN to identify the specific customer account and then forwards that specific account data to merchant systems and records for normal prior art payment transaction processing by the merchant.

What Rose does not teach and the distinguishing feature of the claimed subject matter payment card system is that in the claimed subject matter, a payment card system database that maintains customer bank account data does not return the customer bank data to the merchant ATM/POS and to the merchant systems for creation of a payment authorization record, because an essential aspect of the claimed subject matter is that the claimed payment card system protects the customer id and bank data from the merchant systems themselves, from where it has been subject to theft in the interconnected systems of the Internet and via other ways, based on many news items in the last many years.

The next major cited prior art is Campisano. This prior art is very similar to Rose, except in Campisano, instead of a payment card or a bankcard, a customer identifier in the form of customer's telephone number is used by entering that in the ATM/POS. Campisano art is on a card-less payment system for credit card transactions. To be able to provide a card-less payment system that does not use a credit card, Campisano teaches a card-less payment system that uses an entry of the user's telephone number combined with a PIN, in lieu of his/her physical bankcard at a point of sale terminal. The telephone number and the PIN are linked to the card number in a card database that may be maintained by the card-issuing bank or the telephone company, as they have the ability to verify the telephone number. The actual bankcard data from the card database is then transferred to the merchant systems for the merchant to process a payment transaction.

The Rose and Campisano prior art, individually and in combination while teach convenience in use of bankcards and protection of customer data on the bankcard itself and teach use of a remote database that maintains customer bank account data, referenced by a customer identifier that would be on the pseudo bankcard, they do not teach or even fairly suggest under the Graham v. Deere obviousness enquiry and analysis, the claimed subject matter which accomplishes a very different objectives, that of security from theft of the customer data from the merchant computer systems themselves.

Before Appellant responds to each of the various obviousness rejections, appellant would first address the KSR and Graham ordinary skill in the art obviousness enquiry argument, given these cited prior art to one of ordinary skill in the art.

As a matter of general knowledge and related to the ordinary skill in the art enquiry that is related to bankcard driven payments systems, a bankcard payment infrastructure, requires that the bankcard data from the customer that includes customer identity data such as name, card expiration and bank name and account number be transferred over to merchant computer systems and records via a merchant point-of-sale (POS) interface. After the bankcard data has been transferred or read into the merchant computer systems, a payment authorization request record is created by the merchant computer systems. That payment authorization request record combines in this payment authorization request record, (i) the customer bankcard data (ii) a payment amount, (iii) merchant identifier, and (iv) transaction identifiers, or meta data such as date, time, and reference number.

This payment authorization request record is then sent or routed to a card-issuing bank via a card authorization network for processing and approving a payment transaction from the customer to the merchant. These prior arts Rose and Campisano cited by the examiner use the same bankcard payment infrastructure and by necessity copy the customer data to the merchant systems.

Rose and Campisano prior art underlie all of the various obviousness rejections. Therefore, these prior arts are examined in detail first for the obviousness and ordinary skill in the art enquiry issue.

In claim 106, elements (b), (c) and (e) are neither taught nor even fairly suggested by Rose and Campisano, given Rose and Campisano analysis above.

Hence under the nature and scope of the claims and in view of ordinary skill in the art, claim 106 cannot be obvious over this cited art.

In claim 109, elements (b) and (c) are neither taught nor even fairly suggested by Rose and Campisano, given Rose and Campisano analysis above. Hence under the nature and scope of the claims and in view of ordinary skill in the art, claim 109 cannot be obvious over this cited art.

In claim 114, elements (b) is neither taught nor even fairly suggested by Rose and Campisano, given Rose and Campisano analysis above. Hence under the nature and scope of the claims and in view of ordinary skill in the art, claim 114 cannot be obvious over this cited art.

In claim 123, element (c) is neither taught nor even fairly suggested by Rose and Campisano, given Rose and Campisano analysis above. Hence under the nature and scope of the claims and in view of ordinary skill in the art, claim 123 cannot be obvious over this cited art.

First, In contrast to the cited prior art, the claimed subject matter independent claims 106, 109, 114 and 123 teach a payment card system with a customer identifier, that is, first without customer identity data and then second, that customer identifier is encoded by reference to an algorithm to make even the customer identifier to be not on the card itself, but an encoded customer identifier, encoded in a specific manner that embeds a reference to an algorithm after the customer identifier is encoded with this specific algorithm.

These above described features related to protecting even a customer identifier without identity data, not relate to a customer in the database are not obvious over the cited art and would not have been obvious to those with ordinary skill in the art as those with the ordinary skill in the art were providing convenience in use of bankcards and not additional security of an already anonymous customer

identifier without customer identity with a reference to a coding algorithm maintained in the database, that codes the anonymous customer identifier on the card itself before encoding it on the card and before delivery of the card to the customer.

To those of the ordinary skill in the art, this additional security measure as applied to the already anonymous customer identifier on the pseudo prior art bankcards serves no purpose as this measure is directed to security in the payment card system.

Second, in contrast, the current application claims 106, 109, 114, 123 and their dependent claims, protect the customer id data from theft and misuse from the merchant computer systems themselves, while enabling a payment transaction with the help of the same merchant computer systems, including the existing POS interfaces, by not transferring customer identity and bankcard data to merchant computer systems in the first place.

This is accomplished by an adapted prior art merchant gateway. A prior art merchant gateway is simply a router or a router mechanism that routes payment authorization requests from merchants globally to the card authorization network globally based on the first four digits of a bankcard number and routes the corresponding payment approval records from the card authorization network to the merchants. The claimed subject matter teach modification or adaptation of that prior art merchant gateway to accomplish the objectives of the claimed subject matter.

The adapted prior art merchant gateway operates, (i) to receive a payment authorization request record from a merchant (ii) filter a payment card originated payment transaction record from other bankcard driven payment transaction records, (iii) temporarily hold the payment card originated transaction record in hold status and route from this transaction, only the encoded customer identifier and the CPIN to a payment card system, (iv) receive from the payment card system the actual customer bankcard data, (v) then assemble a payment authorization request

record with the actual customer bankcard data and (vi) end the hold by submitting this assembled payment authorization request record to a card authorization network and receive a payment authorization approval record from the card-issuing bank, and (vii) forward the payment approval record received from the card-issuing bank to the merchant systems.

While the steps (ii) to (v), as above define the specific adaptation of the prior art merchant gateway, including its interface to the payment card system, the steps (i) and (vii) do not alter existing merchant system interface to this adapted prior art merchant gateway and step (vi) does not alter the existing interfaces of the adapted prior art merchant gateway to the card authorization network.

Hence, the adapted prior art merchant gateway, as described above, is transparent in its operation to the merchants and the card authorization network, while protecting the customer identity and bankcard data from the merchant systems.

Those with the ordinary skill in the art at that time were not solving the issue of keeping the customer bankcard data from theft and misuse in the merchant computer systems themselves, and these prior art do not teach or fairly suggest to one of the ordinary skill in the art, that the customer data having being received by the Merchant POS is subject to theft from these systems and need to be protected from the merchant systems themselves, as in addition to the merchant misusing the customer data, the data may be subject to theft from the interconnected via internet merchant computer systems as has been covered in many news stories, since the current application was filed.

The theft of data from the merchant computer systems was an issue that did not exist for those of the ordinary skill in the art, as their effort was directed for making improvements in the bankcard itself and improvements in the merchant

POS, and it was not directed to protecting bankcard customer identity data against theft and misuse from the merchant computer systems themselves.

Given that these cited prior art in any combination did not alter or change the underlying bankcard driven payment mechanism, as described earlier, from these prior art citations, the ordinary skills in the art pertain to computer networks, databases, and systems, specifically for the payment systems that includes the use of bankcards. To them, the issue of protecting the customer identity data from theft and misuse from the merchant computer systems was not an issue and thus not obvious as an issue to be addressed.

The claimed subject matter, while using the same merchant point of sale interfaces and merchant computer systems do not transfer customer identity data to these same merchant computer systems, a novel and non-obvious accomplishment in itself and over the cited art. And this cited art to those with ordinary skill in the art, for the reasons as detailed above does not make obvious the protection of the customer identity and bankcard data from theft and misuse from the merchant computer systems themselves.

Second, in contrast the merchant gateway adapted to perform the function of a logic to separate payment cards from a bankcard and then interfacing with a payment card system to fetch customer bankcard data and then assembling a complete payment auth request record are neither taught or even fairly suggested in the cited prior art.

Now analyzing other cited prior art: Low et al is a very different art in how it accomplishes its stated objective of anonymous credit card transactions. Analyzing Low et al, Low teaches anonymous credit card transactions without disclosing the subject matter of the transaction to the institution providing the credit card (from Low Abstract).

From Low Figure 2, col. 3, lines 21 to col. 4, lines 24, Low creates two independent card-issuing bank entities, identified as Bc 203 and Bp 213, where Bc knows the customer identity and issues the anonymous card, and Bp, the bank that only manages money or credits that have been deposited in the account, and only knows the customer by a anonymous identifier. These pseudo banks Bc and Bp interface with each other via an intermediary central bank Cx and the merchant bank Bs 237 via the same intermediary central bank Cx 227. The central bank Cx exchanges messages between Bc, Bp and Bs using public key cryptography, without each of them knowing the true identity of each other but only a cryptographic identity, where each bank uses a cryptographic identification. Bc sends messages to Bp via Cx to transfer funds or credits and Bp sends messages to Bs via Cx to transfer funds.

Low for its operation requires a smart card as it stores Bp cryptographic address, receives and stores Bp cryptographic address and fund amount for transferring them to Cx. The crypto address of Bp is already on the anonymous card and the crypto address of the merchant bank and the purchase amount is copied to the card at the merchant sale terminal and the card then transfers these two crypto addresses and the fund amount to the central bank Cx 227 via message 233. This enables the central bank Cx 227 to transfer funds from the bank Bp to merchant bank Bs. When the Bank Bs notifies the merchant S 245, the merchant then releases the goods to the customer.

While Bc may appear to be like current invention payment card system, it is not as Bc creates and sends itemized account statements to the customer, whereas current invention payment card system only delivers the payment card to the customer. Also there is no equivalent of Low's Bp, Cx, smart card, and use of public key cryptography in the current invention. Furthermore, Low would require unique to Low Merchant POS that provide merchant bank's cryptographic identity the credit card of the customer, along with a dollar purchase amount for transfer to the central bank Cx.

Low does not teach features of claim 106 to 124 that use existing merchant POS and merchant systems and existing card authorization networks and an adapted merchant gateway to protect customer id data from the merchant computer systems. Hence Low is wholly different in every aspect from the claimed subject matter. Thus Low does not make obvious any of the independent claims from 106-124, and thus also any of their dependent claims

RESPONSE TO VARIOUS 103(a) OBVIOUSNESS REJECTIONS

Each of the various obviousness rejections is responded to as follows in light of the above arguments.

Claim 106-108 103(a) rejection

Examiner had rejected under 35 USC 103(a) obvious rejections, claims 106 and 108 as being obvious over Rose et al in view of Campisano and further in view of Duyck, and further in view of Low et al.

These claims would not be obvious to those with ordinary skill in the art in view of arguments above related to Rose and Campisano. The additional citations do not teach or fairly suggest, or would be obvious to those with ordinary skill in the art, the features of claims 106 and 108, for the reasons as described above.

Claim 107, 103(a) rejection

Examiner had rejected under 35 USC 103(a) obvious rejections, the claim 107 as being obvious over Rose et al in view of Campisano, in view of Duyck, and further in view of Low et al, and further in view of Kramer...

These claims would not be obvious to those with ordinary skill in the art in view of arguments above related to Rose and Campisano. The additional citations do not teach or fairly suggest, or would be obvious to those with ordinary skill in the art, the features of claim 107 for the reasons as described above.

Claim 109-110, 114, and 123, 103(a) rejection

Examiner had rejected under 35 USC 103(a) obvious rejections, claims 109-110, 114 and 123 as being obvious over Rose et al.

These claims would not be obvious to those with ordinary skill in the art in view of arguments above related to Rose and Campisano. The additional citations do not teach or fairly suggest, or would be obvious to those with ordinary skill in the art, the features of claims 109-110, 114 and 123 for the reasons as described above.

Claim 112, 115-116, 103(a) rejection

Examiner had rejected under 35 USC 103(a) obvious rejections, claims 112, 115-116 as being obvious over Rose et al in view of Campisano.

These claims would not be obvious to those with ordinary skill in the art in view of arguments above related to Rose and Campisano. The additional citations do not teach or fairly suggest, or would be obvious to those with ordinary skill in the art, the features of claims 112, 115-116 for the reasons as described above.

Claim 111, 103(a) rejection

Examiner had rejected under 35 USC 103(a) obvious rejections, claims 111, as being obvious over Rose et al as applied to claim 109 and further in view of Campisano.

These claims would not be obvious to those with ordinary skill in the art in view of arguments above related to Rose and Campisano. The additional citations do not teach or fairly suggest, or would be obvious to those with ordinary skill in the art, the features of claims 111 for the reasons as described above.

Claim 113, 103(a) rejection

Examiner had rejected under 35 USC 103(a) obvious rejection, claims 113, as being obvious over Rose et al as applied to claims 109, 112 and further in view of Campisano and Low et al.

These claims would not be obvious to those with ordinary skill in the art in view of arguments above related to Rose and Campisano. The additional citations do not

teach or fairly suggest, or would be obvious to those with ordinary skill in the art, the features of claim 113 for the reasons as described above.

Claim 117, 103(a) rejection

Examiner had rejected under 35 USC 103(a) obvious rejection, claims 117, as being obvious over Rose et al as applied to claims 114-116 and further in view of Low et al.

These claims would not be obvious to those with ordinary skill in the art in view of arguments above related to Rose and Campisano. The additional citations do not teach or fairly suggest, or would be obvious to those with ordinary skill in the art, the features of claim 117 for the reasons as described above.

Claim 118-120, 103(a) rejection

Examiner had rejected under 35 USC 103(a) obvious rejection, claims 118-120, as being obvious over Rose et al as applied to claims 114 and further in view of Albert et al and Duyck.

These claims would not be obvious to those with ordinary skill in the art in view of arguments above related to Rose and Campisano. The additional citations do not teach or fairly suggest, or would be obvious to those with ordinary skill in the art, the features of claims 118-120 for the reasons as described above.

Claim 121, 103(a) rejection

Examiner had rejected under 35 USC 103(a) obvious rejection, claims 121, as being obvious over Rose et al as applied to claims 114 and further in view of Albert et al and Duyck as applied to claims 118-120 above and further in view of Campisano and Gillin et al.

These claims would not be obvious to those with ordinary skill in the art in view of arguments above related to Rose and Campisano. The additional citations do not teach or fairly suggest, or would be obvious to those with ordinary skill in the art, the features of claim 121 for the reasons as described above.

Claim 122, 103(a) rejection

Examiner had rejected under 35 USC 103(a) obvious rejection, claims 122, as being obvious over Rose et al as applied to claims 114 and further in view of Albert et al and Duyck as applied to claims 118-120 above and further in view of Campisano and Gillin et al as applied to claim 121 above and further in view of Low et al.

These claims would not be obvious to those with ordinary skill in the art in view of arguments above related to Rose and Campisano. The additional citations do not teach or fairly suggest, or would be obvious to those with ordinary skill in the art, the features of claims 122, 114, 118-120, and 121 for the reasons as described above.

Claim 124, 103(a) rejection

Examiner had rejected under 35 USC 103(a) obvious rejections, claims 124, as being obvious over Rose et al as applied to claims 123 above and further in view of Campisano and Low et al.

These claims would not be obvious to those with ordinary skill in the art in view of arguments above related to Rose and Campisano. The additional citations do not teach or fairly suggest, or would be obvious to those with ordinary skill in the art, the features of claim 124 for the reasons as described above.

GROUND #2

Examiner misunderstands and mis-cites KSR v. Teleflex, and its seven rationales to support 103 (a) rejections, under an obviousness enquiry.

Appellant's Arguments:

KSR did not change Graham v. Deere, the applicable law of obviousness, but clarified the application of Graham V. Deere test of obviousness, in those obviousness enquiry cases that combine known elements according to known methods that yield predictable results that are in the purview of those with ordinary skill in the art.

The claimed subject matter do not provide known elements according to known methods as the scope of claims and the prior art cited by the examiner make it clear that those with ordinary skill in the art at that time were focused on providing convenience in use of bankcards and prevent theft of bankcards from the customer's possession. The prior art of record shows that those with the ordinary skill in the art at that time were not trying to provide security by protecting the bankcard identity data from the merchants and merchant sale systems themselves. Security of bankcard data from the merchants themselves due to theft and compromise from their systems was not an issue to be solved in year 2001 in the purview of those with ordinary skill in the art at that time.

Therefore, Applicant submits that the claims 106 to 124 are not obvious over these prior arts, where these prior art individually or in any combination do not teach or suggest the invention in these claims and would not be obvious to those of ordinary skill at that time.

GROUND #3:

Examiner misconstrues and mis understands the nature and scope of the claimed subject matter" as used in the claims in light of the specification and thus has erred in applying the "Broadest reasonable construction" standard and as a basis for 103(a) obviousness rejection.

Appellant's Arguments:

Examiner by equating claim phrase "adapted prior art merchant gateway with a merchant system" as used in the claims in light of the specification has erred in applying the "Broadest reasonable construction" standard and as a basis for 103(a) obviousness rejection.

Examiner by equating claim phrase "a customer identifier, without customer identity data, and a payment card that encodes the customer identifier" as used in the claims in light of the specification with prior art encoding of customer identity data in the magnetic strip, and thus has erred in applying the "Broadest reasonable construction" standard and as a basis for 103(a) obviousness rejection.

The Patent and Trademark Office ("PTO") determines the scope of claims in patent applications not solely on the basis of the claim language, but upon giving claims their broadest reasonable construction "in light of the specification as it would be interpreted by one of ordinary skill in the art." *In re Am. Acad. of Sci. Tech. Ctr.*, 367 F.3d 1359, 1364[, 70 USPQ2d 1827] (Fed. Cir. 2004).

Examiner misconstrues and mis understands the nature and scope of the claimed subject matter" as used in the claims in light of the specification and thus has erred in applying the "Broadest reasonable construction" standard and as a basis for 103(a) obviousness rejection.

Examiner by equating claim phrase "a customer identifier, without customer identity data, and a payment card that encodes the customer identifier" as used in the claims in light of the specification with prior art encoding of customer identity

data in the magnetic strip, and thus has erred in applying the "Broadest reasonable construction" standard and as a basis for 103(a) obviousness rejection.

Examiner by equating claim phrase "adapted prior art merchant gateway with a merchant system" as used in the claims in light of the specification has erred in applying the "Broadest reasonable construction" standard and as a basis for 103(a) obviousness rejection.

Hence, the scope and content of prior art and the differences between the claimed invention and the prior art are such that the current invention has an entirely different scope than the prior art.

(8) CLAIMS APPENDIX

Claims involved in this appeal are:

Claims 1 to 105 (cancelled)

106. A method of protecting from theft and misuse bankcard data from merchant computer systems and securely selecting any one of a plurality of bankcards of a customer at a merchant point of sale interface for a payment transaction to a merchant comprising the steps of:

a. enabling selecting a debit card transaction requiring entry of a PIN in a merchant point of sale (POS) interface, enabling entering of (i) a customer identifier, without customer identity data, by a payment card that encodes the customer identifier and (ii) a bankcard specific personal identification number (CPIN) in the merchant point of sale (POS) interface;

b. enabling sending the customer identifier and the CPIN to an adapted prior art merchant gateway, along with the payment transaction data that includes a merchant identifier and a payment amount;

c. interfacing by the adapted prior art merchant gateway with a payment card system, and sending to the payment card system the customer identifier and the CPIN;

d. having stored customer bankcard data in the payment card system, wherein, each bankcard is identified with a separate CPIN, identifying a particular bankcard data of the customer and verifying the customer by the bankcard specific CPIN in the payment card system;

e. returning to the adapted prior art merchant gateway the bankcard data corresponding to the customer identifier and the CPIN from the payment card system;

f. assembling by the adapted prior art merchant gateway, a payment transaction record to include the bankcard data from the payment card system and the payment transaction data, and by submitting the payment transaction record to a

bankcard authorization network, wherein the method does not transfer bankcard identity data to the merchant computer systems.

107. The method as in claim 106, comprising further steps of:

encoding the customer identifier without customer identity data on the payment card with an algorithm and decoding the customer identifier with the algorithm in the payment card system to get the customer identifier.

108. The method as in claim 106, comprising further steps of:

a. delivering the payment card to the customer;

b. enabling entering the bankcard data and self-selecting a CPIN for each of the bankcards of the customer in the payment card system.

109. A payment card system and that protects private data of a customer from theft and misuse from merchant computer systems in customer to merchant payment transactions, comprising:

a. a payment card with a substrate;

b. a customer identifier that is without customer identity data, the customer identifier maps to the payment card system;

c. the customer identifier is encoded to be an encoded customer identifier when the customer identifier is encoded with an algorithm in the payment card system and then embeds a reference code that references the algorithm;

d. the substrate encoded with the encoded customer identifier and the substrate printed with an alias name selected by the customer.

110. The payment card system as in claim 109, comprising:

the encoding medium is a magnetic strip.

111. The payment card system as in claim 109, comprising:

the customer-identifier is self-created by the customer.

112. The payment card system as in claim 109, further comprising:

a. the encoded customer identifier from the payment card used for a payment transaction at a merchant point of sale (POS), along with entry of a bankcard specific personal identification number (CPIN) by the customer are routed from the POS to an adapted prior art merchant gateway, the adaptation in the prior art merchant gateway routes the encoded customer identifier and the CPIN to the payment card system;

b. the payment card system decodes the encoded customer identifier using the algorithm that is referenced by the code present in the encoded customer identifier, the payment card system then maps the customer identifier and the CPIN to retrieve a specific bankcard data and returns the specific bankcard data to the adapted prior art merchant gateway.

113. The payment card system as in claim 112, further comprising:

the adapted prior art merchant gateway, after receiving the specific bankcard data from the payment system, assembles a payment transaction record using the specific bankcard data for submission of the payment transaction record to a bankcard authorization network, thereby the payment card operating with the payment card system does not transfer customer identity data to the merchant computer systems.

114. A method of conducting a payment transaction that protects the privacy of customer identity and bankcard data, from theft and misuse from merchant computer systems, comprising the steps of:

a. enabling creating a customer identifier that is without customer identity data, the customer identifier maps to a payment card system;

b. encoding the customer identifier with an algorithm, and then embedding a reference code that references the algorithm in the payment card system, thus getting an encoded customer identifier;

c. delivering to a customer, a payment card with a substrate printed with an alias name selected by the customer and encoded with the encoded customer identifier.

115. The method as in claim 114, further comprising the steps of:

a. enabling using the payment card for the payment transaction at a merchant point of sale (POS) and entering a bankcard specific personal identification number (CPIN) by the customer;

b. enabling the POS routing a payment transaction record to an adapted prior art merchant gateway;

c. enabling identifying the use of the payment card at the POS, by the adapted prior art merchant gateway, and routing the encoded customer identifier and the CPIN of the payment transaction to the payment card system.

116. The method as in claim 115, further comprising the steps of:

decoding the encoded customer identifier by the payment card system using the algorithm that is referenced by the code in the encoded customer identifier, and using the customer identifier and the CPIN, retrieving specific bankcard data in the payment card system, and returning to the adapted prior art merchant gateway.

117. The method as in claim 116, further comprising the steps of:

enabling the adapted prior art merchant gateway, after receiving the specific bankcard data from the adapted prior art merchant gateway, to assemble a payment transaction record with the specific bankcard data for submitting the payment transaction record to a bankcard authorization network, wherein the payment card does not transfer customer identity data to the merchant computer systems.

118. The method as in claim 114, further comprising the steps of:

a. enabling using the payment card for the payment transaction at a merchant point of sale (POS) and enabling entering a bankcard specific personal identification number (CPIN) by the customer;

b. connecting wirelessly by the merchant POS to the payment card system for routing a payment transaction record that includes a payment amount, a merchant identifier, a reference number, the encoded customer identifier, and the CPIN.

119. The method as in claim 118, further comprising the steps of:

receiving wirelessly the payment transaction record by the payment card system.

120. The method as in claim 119, further comprising the steps of:

decoding the encoded customer identifier by the payment card system using the algorithm that is referenced by the code in the encoded customer identifier, and using the customer identifier and the CPIN, retrieving specific bankcard data in the payment card system.

121. The method as in claim 120, further comprising the steps of:

assembling a payment transaction record with the specific bankcard data, the payment transaction record includes, a customer name, a bankcard number, an expiration date, the merchant identifier, the payment amount, and the reference number, and submitting the payment transaction record to a card authorization network via an adapted prior art merchant gateway.

122. The method as in claim 121, further comprising the steps of:

receiving a payment approval record by the payment card system from the card authorization network via the adapted prior art merchant gateway, the payment approval record includes the reference number, the payment amount and a payment authorization number, and forwarding wirelessly the payment approval record to the

merchant POS, wherein the payment card does not transfer customer identity and bankcard data to the merchant computer systems.

123. A payment security system that provides identity security in use of bankcards, from merchant computer systems, comprising:

a. a customer identifier that is without customer identity data;

b. the customer identifier maps to a plurality of bankcard data of the customer, each bankcard data identified with a card specific personal identification number (CPIN) in the payment security system;

c. the customer identifier is encoded to be an encoded customer identifier when encoded with an algorithm from a list of such algorithms in a database maintained by the payment security system and then embeds a reference code that references the algorithm, the encoded customer identifier is then encoded on a payment card encoding mechanism, wherein the payment card and the CPIN is used by the customer at a merchant point of sale (POS) of a merchant system for conducting a payment transaction.

124. The payment security system as in claim 123, further comprising:

on swiping of the payment card and entry of the CPIN, the payment security system receives from the merchant POS, the encoded customer identifier and the CPIN, decodes the encoded customer identifier, using the customer identifier and the CPIN selects the specific bankcard data of the customer for processing the payment transaction with a bankcard processing network, wherein, the security system does not transfer the customer identity and customer bankcard data to the merchant computer systems.

(9) EVIDENCE APPENDIX

None

(10) RELATED PROCEEDINGS APPENDIX

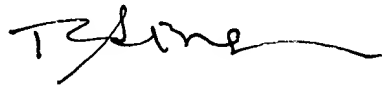
None

CONCLUSION

Appellant submits, based on the arguments presented in this appeal, the current claimed subject matter is entirely of a different scope and the current claims 106-124 are not obvious under section 35 USC 103(a) and Graham v. Deere test over the cited combination of the prior art, based on arguments presented in this appeal.

Dated this the 29th day of March, 2010

Respectfully submitted,



Tara Chand Singhal
Appellant

P O Box 5075
Torrance, California 90510
Telephone: (310) 540-4095